DISCOVERY

To Cite:
Kamugisha GW, Mshana JA. Perception on cyber security threats upon using social media: Perspectives from postgraduate students from the Institute of Accountancy Arusha (IAA) Dar es Salaam Campus. *Discovery* 2023; 59: e104d1310

Author Affiliation:
[1]Department of Informatics, Institute of Accountancy Arusha, Tanzania
Email: gmodestus2020@gmail.com
[2]Senior Lecturer, Department of Informatics, Institute of Accountancy Arusha, Tanzania
Email: jumamshana@gmail.com

Peer-Review History
Received: 08 June 2023
Reviewed & Revised: 12/June/2023 to 18/July/2023
Accepted: 22 July 2023
Published: August 2023

Peer-Review Model
External peer-review was done through double-blind method.

Discovery
pISSN 2278–5469; eISSN 2278–5450

Perception on cyber security threats upon using social media: Perspectives from postgraduate students from the Institute of Accountancy Arusha (IAA) Dar es Salaam Campus

Glory William Kamugisha[1], **Juma Ally Mshana**[2]

ABSTRACT

This study aimed to assess the student's perception of cyber security threats when using social media. The study employed communication privacy management theory. This study was conducted at the Institute of Accountancy Arusha – Dar es Salaam Campus where the target population was 382 from which a sample size of 195 was obtained to represent postgraduate students. The study employed quantitative research approach and descriptive research design; upon which data was collected through a questionnaire. The collected data was analyzed by using SPSS Version 25 which enabled the research to perform different statistical tests such as descriptive statistics, correlation analysis and regression analysis to assess the students' perception of cyber security threats. The finding of this study revealed that, students are aware of cyber security threats they face when using social media. The study therefore recommends that students should be given regular cyber security training to promote the security of social media consistently. It was also recommended that social media owners should keep communication lines open to the social media user to report, communicate and remind the service provider of the presence of any security breach. Lastly students should ensure that they do not become negligent or reckless when dealing with social media.

Keywords: Cyber security threats, social media, IAA, students' perception, cyber security awareness

1. INTRODUCTION

The use of social media in daily life has become inevitable. People, companies, organizations and even governments use different social media platforms to share information and disseminate news. It was estimated that there were 4.65 billion social media users around the world by May 2022 (Data Reportal, 2022), equal to 58.7 percent of the total global population (Kemp, 2022). The average

social media user engages with an average of 6.6 on numerous social media platforms. According to Data Reportal, (2022), there are 2.912 billion monthly active users of Facebook, 2.562 billion users of YouTube, and 2 billion active users of WhatsApp and Instagram's potential advertising reach is 1.452 billion.

The widely use of social media has increased in volume, velocity and variety of data in networking hence leading to the rising of several social concerns including security and privacy issues (Ghosh and Nath, 2016). The rapid growth of these tools has opened doors to cybercriminals exploiting security vulnerabilities on the internet. This has resulted in different types of cyber-criminal activities with users becoming the main target in social networks through the platform system design. There is an increase in Cyber security related issues due to the growth of the internet and social media usage in Africa.

Social media platforms are so desired by cyber-criminals because these sites make it easy to share anything including Malware (Lindsey, 2019). Also, these platforms allow anyone to register without much security checks for instance user true identity; this has resulted in the growing number of bots and ghost accounts that conducts criminal activities. The use of social media is prevalent in both the general society and university students. People who use such platforms in all wakes of their lives are often exposing highly sensitive personal information without realizing the consequences of data misuse. Thus, security and confidentiality issues in online social networks are now increasing and becoming riskier (Krubhala et al., 2015).

Social media might be a risk to information security because users are not aware of the risks and threats. Lack of cyber security awareness is one of the major problems identified by various researchers that increase cyber security threats and concerns (De-Bruijn and Janssen, 2017). There are many things to be aware of such as social engineering risks, baits, scammers, malware, fake users and misusing of information. These are negative aspects of social networking related to information security which is taking place from user usage, or design issues related to privacy and security.

College students are among the most users of social media platforms, who use them mainly for two major activities, education and socializing (Senthilkumar and Easwaramoorthy, 2017). The impact of their security awareness is significant and far-reaching for society. Hence, this study was conducted to assess the perception of students on cyber security threats when using social media platforms. And hence, to uncover the cyber security awareness of the students as it pertains to security on social media platforms.

Literature Review

There is misconception and widespread of belief to the people about cyber security issues. Some people believe that cyber-criminals' focus on the big business and celebrities and not the ordinary people; another belief is that there are few consequences of being a victim of cybercrime. Also, there is an array of inconsistent advice given to people that leads to dangerous inertia (Britainthinks, 2022). According to Kostyuk and Wayne, (2019), cases of identity theft do not receive broad attention and coverage in the news hence most of the people believe that they are not personally likely to be targeted by hackers. Thus, the way the public thinks about cybercrimes and the reality of the threats has caused a significant perception gap. This gap is based on the myth such as cybercrimes are not the concern of many users of information systems; others have the perception that cybercrimes are not real while other thinks that they can do nothing to ensure their protection.

Neelima, (2020) examined the students' perceptions on the social media risk and their knowledge of the user personal privacy and security of the information system in the social media application. In this study the survey techniques were used in the regional campuses in Pennsylvania. The findings of this study show that students have awareness on the privacy and risks on security on the use of social media. Also, results obtained show that training must be provided at this domain.

2. METHODOLOGY

The study involved a quantitative research approach and a descriptive research design which helped the researcher to explore the existing status of students' perception on cyber security threats when using social media in Tanzania. This study was conducted at Institute of Accountancy Arusha – Dar es Salaam Campus, the data was collected by using the questionnaire from 195 respondents among the postgraduate students. The collected data was coded into Statistical Package for Social Sciences (SPSS) and analysed using descriptive statistics, correlation as well as regression analysis

3. RESULTS

The results of the study on the Student's Perception of Cyber Security Threats when using social media were as follows in descriptive statistics, the study presented the minimum, maximum, Mean and Standard Deviation in the examination of the deviations as well as measuring the central tendency of the research variables. The results obtained through descriptive statistics were presented in (Table 1).

Table 1 Students' Perception of Cyber Security Threats when using social media

Descriptive Statistics on Students' Perception of Cyber Security Threat when Using social media	*N*	*Min*	*Max*	*Mean*	*Std. D*
Social media are targeted by security breaches of social engineering	173	2	5	3.97	.999
Posting true details about yourself is high risk	173	1	5	4.20	.992
I can use a virtual private network to avoid being targeted	173	1	5	3.53	1.353
I have a perception that not friend requests should be reviewed before being accepted	173	1	5	3.58	1.334
Knowing the geotags attached to the picture or information being shared on social media	173	1	5	3.94	1.195
Security reminders and updates from time to time can be useful for social media users	173	1	5	3.75	1.178
Regular change of information related to social media account users	173	2	5	4.27	.964
Valid N (list wise)	173				

Source: Authors' own data (2022)

Table 1 revealed that social media are targeted by security breaches of social engineering (Min=2, Max=5, Mean=3.97 and SD=.999). Also posting true details about yourself is highly risk (Min=2, Max=5, Mean=4.20 and SD=.992), also it was revealed that the use virtual private network to avoid being targeted (Min=1, Max=5, Mean=3.53 and SD= 1.353). On the other hand, there was a perception that friend requests should be reviewed before being accepted as shown by (Min=1, Max=5, Max=3.58 and SD=1.334).

Other respondents said that they knew the geotags attached to the picture or information being shared on social media as shown by Min=1, Max=5, Mean=3.94 and SD=1.195, there was a perception of the use of Security reminders and updates time to time can be useful for social media users (Min=1, Max=5, Mean=3.75, SD=1.178), and lastly, students had perception on regular change of information related to social media account users as shown by (Min=2, Max=5, Mean=4.27 and SD=.964). The Pearson correlation was calculated to determine the relationship between the variables as in (Table 2).

Table 2 Correlation Analysis

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.742	.168		22.286	.791
	Individual Perception of Cyber Threats	.191	.039	.419	4.963	.000

Source: Field data (2022)

Table 2 show that an inspection of the individual predictors in the model significant in the model showed a significant relationship between the individual Perception of Cyber Threats (β=-.419, p<000), which means that there is a relationship between perception of cyber threats by the students and awareness of cyber security on the use of social media.

4. DISCUSSION OF FINDINGS

The perception of students about cyber security threats when using social media based on the results obtained through descriptive statistics in Table 1, suggests that the determinant of the student's perception about cyber security such as social media are targeted by security breaches of social engineering, posting true details about yourself is high risk and the use a virtual private network to avoid being targeted. Also, perceptions that friend requests should be reviewed before being accepted, knowing the geotags (geographic location) attached to the picture and information being shared on social media, security reminders and updates from

time to time can be useful for social media users as well as regular change of information related to social media account users were found to have higher mean values and standard deviation values.

These findings are highly supported by Neelima, (2020) who also established that individual perception of the students about cyber security threat is very important when using social media. Also, it was revealed those students' perceptions of personal social media risks and their knowledge of the use for privacy and security setting in social media application is high. Table 2 have shown that individual perception of cyber threats had 0.00 level of significance which means that there is a positive significant relationship with awareness of cyber security in the use of social media. This was also reported in the study conducted by Richardson, (2017); the perception of the use of social media on the security of their information is important and it was shown that 70% of the students who use social media service conduct user checks of their accounts multiple times a day.

5. CONCLUSION AND RECOMMENDATION

The objective of this study was to assess student perception of cyber security threats when using social media. This study revealed that through descriptive statistics various aspects related to students' perception of cyber security as depicted by the results such as the perception that social media are targeted by security breaches of social engineering as shown by Mean=3.97 and SD=.999, also others perceived that posting true details about yourself is high risk as shown by a Mean=4.20 and SD=.992, another perception was that the use virtual private networks to avoid being targeted as shown by a Mean=3.53 and SD=1.353, another perception was that friend requests should be reviewed before being accepted Max=3.58 and SD=1.334, also it was important to know the geotags attached to the picture or information being shared in social media as shown by a Mean=3.94 and SD=1.195. on the other hand, the use of security reminders and updates from time to time can be useful for social media users shown by Mean=3.75, SD=1.178, also, there was a perception of regular changes in information related to social media account users which had a Mean=4.27 and SD=.964.

From these results, it is generally concluded that postgraduate students recognize the presence of cyber security threats when using social media. And thus, they are aware of different cyber security threats that are present in on social media platforms and what kind of actions or shared information can put them at risk and make themselves targets for cyber criminals. Since social media has become the desired medium of communication for billions of web users, the study recommends a state-of-the-art study on several kinds of privacy and security issues in social media that arise from some of their significant features such as sharing personal information and commenting.

Also, the study generally recommends that social media users should be careful about what they choose to post and share on social media not reveal sensitive personal information, or financial information because cyber criminals frequently leverage publicly accessible social media information to tailor their attacks. The government and other related institutions should focus on policy development and public awareness campaigns to sensitize the public on how to utilize social media platforms in a well-protected and secured manner to reduce the risks of cyber-attacks.

Informed consent

Not applicable.

Ethical approval

Not applicable.

Conflicts of interests

The authors declare that there are no conflicts of interests.

Funding

The study has not received any external funding.

Data and materials availability

All data associated with this study are present in the paper.

REFERENCES AND NOTES

1. Britainthinks. A call to action: The Cyber Aware Perception Gap 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/684609/BT_CYBER_AWARE_V11_280218.pdf

2. Data Reportal. Digital 2022: Global Digital Overview 2022. https://datareportal.com/reports/digital-2022-global-overview-report
3. De-Bruijn H, Janssen M. Building cyber security awareness: The need for evidence-based framing strategies. Gov Inf Q 2017; 34(1):1-7.
4. Ghosh K, Nath A. Big data: Security issues and challenges. Int J Res Stud Comput Sci Eng 2016; 1-9.
5. Kostyuk N, Wayne C. Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats 2019.
6. Krubhala P, Niranjana P, Priya GS. Online Social Network-A Threat to Privacy and Security of Human Society. Int J Sci Res Publ 2015; 5(4):1-6.
7. Lindsey N. Cyber Criminals Have Turned social media Cyber Crime Into a $3 Billion Business 2019. https://www.cpomagazine.com/cyber-security/cyber-criminals-have-turned-social-media-cyber-crime-into-a-3-billion-business/
8. Neelima B. Students attitudes, awareness and perception of personal privacy and cybersecurity in using social media; an initial study. Int Syst Educ J 2020; 18(1):48–57.
9. Richardson C. Student perceptions of the impact of social media on college student engagement (Doctoral Thesis) 2017. https://scholarcommons.sc.eduent?
10. Senthilkumar K, Easwaramoorthy S. A Survey on Cyber Security awareness among college students in Tamil Nadu. In IOP Conference Series: Materials Science and Engineering. IOP Publishing 2017; 263(4):042043.